

ESCRITURA ENCRIPTADA

La necesidad de comunicarnos con nuestros semejantes y de transmitir conocimientos, hechos o informaciones ayudó al desarrollo de la escritura. La escritura permitía la comunicación a la vez que surgía la necesidad de que los mensajes solo llegaran a las personas adecuadas y no estuvieran disponibles para todo el mundo.

Por ello aparecieron los primeros sistemas de escritura encriptada. Civilizaciones como la mesopotámica, india o china desarrollaron sus propios sistemas de encriptación a lo largo de la historia como por ejemplo la ¹escítara, el código de ²sustitución de letras, el ³tratado de cifras hasta llegar al tratado de criptografía moderna ideado por Johannes Trithemius (1530).

La finalidad principal de la criptografía moderna ha sido militar pero después ha servido a diferentes finalidades y en la actualidad es fundamental en la web.

A continuación te proponemos varias actividades en las que aprenderás a utilizar distintos códigos para descifrar mensajes, cifrar los suyos propios y crear sus propios sistemas de cifrado.



¹ Sistema de criptografía utilizado por los éforos espartanos para el envío de mensajes secretos.

² Se escribía el documento codificado con la tercera letra que siguiera a la que realmente correspondía. Sistema ideado por Julio César

³ En 1470, León Battista Alberti publica "Tratado de cifras" en donde describe una cifra capaz de encriptar un pequeño código.

PARA EL ALUMNADO: MENSAJES ENCRIPTADOS

Actividad. Lee el siguiente texto.

En numerosas películas hemos visto cómo el o la protagonista de la misma debe descifrar un mensaje oculto para salvar a alguien y vencer al villano. Los mensajes ocultos no solo son propios del cine.

La criptografía se define como la técnica que se ocupa de alterar o modificar los mensajes con el fin de que solo puedan ser legibles para algunas personas.

La criptografía es casi tan antigua como la escritura. Su historia comenzó hace miles de años. Existen ejemplos de escritura encriptada en las tumbas de Egipto. En Esparta también se utilizaban los mensajes cifrados para hacer llegar las órdenes a los generales sin que pudieran ser descubiertos. El sistema utilizado era la "**Escítala espartana**", que consistía en enrollar un papiro en forma de espiral alrededor de un bastón o cilindro.

Otro sistema utilizado consistía en escribir sobre tablillas de madera y cubrir después los textos con cera para hacerlos desaparecer.

¿Conoces la historia de Histieo de Mileto?

En la antigua Grecia Histieo fue apresado por los persas en Susa. Histieo quería hacer llegar un mensaje secreto a su padre, Aristágonos, para que atacara a los persas, sin que nadie pudiera interceptarlo. Para hacerlo se le ocurrió la siguiente idea: afeitó y tatuó la piel de la cabeza de uno de sus más fieles soldados y esperó a que le creciera de nuevo el pelo. Luego escribió a su padre un mensaje inocente para no levantar las sospechas de sus captores. Cuando el soldado se presentó ante Aristágonos volvió a afeitarse su cabeza y le mostró el mensaje real.

Julio César utilizaba un código secreto que consistía en sustituir cada letra del mensaje por otra que en el alfabeto estuviera desplazada tres lugares. Leonardo da Vinci escribía sus estudios con anotaciones al revés para encriptarlas.

Como vemos al principio se utilizaban sistemas muy sencillos utilizando diferentes soportes y luego con sistemas mecánicos sencillos que con el tiempo se fueron haciendo más complejos, como la máquina de rotores Enigma hasta el cifrado actual que utiliza métodos de cifrado muy sofisticados.

Enigma era el nombre de una máquina que disponía de un mecanismo de cifrado rotatorio, que permitía usarla tanto para cifrar como para descifrar mensajes.

Alan Turing lideró el grupo de criptoanalistas británico que consiguió descifrar los mensajes alemanes que usaban la máquina durante la II Guerra Mundial.

Para ello creó un sistema de criptoanálisis y participó en el diseño y construcción de Colossus lo que muchos consideran el primer ordenador de la historia. Colossus fue obra del propio Turing y de Bill Tutte.

Sus trabajos permitieron descifrar la mayoría de los mensajes que transmitían los alemanes.

Pero a día de hoy, no todos los mensajes han podido ser resueltos, actualmente se conservan códigos que no han podido ser descifrados como el Disco de Festo y El manuscrito Voynich, un libro ilustrado con textos y dibujos que no han podido ser todavía desvelados.

Para tener éxito en el cifrado de mensajes es necesario que la persona que lo escribe y el destinatario del mismo conozcan el código secreto utilizado.

Antes de empezar a descifrar y codificar mensajes vamos a conocer el vocabulario utilizado por los "espías" que los utilizan:

- Texto plano: es el mensaje escrito tal cual, sin modificar.
- Texto cifrado: es el mensaje alterado o codificado (encriptado)
- Código o algoritmo: lo que hacemos para transformar el mensaje
- Cifra: es el método utilizado para transformar el mensaje.
- Clave: una ayuda que nos permite descifrar el mensaje de forma más rápida.

Vamos a ver algunos ejemplos:

CÓDIGO: CAMBIAR EL ORDEN DE LAS LETRAS EN CADA PALABRA

- Texto plano: MAÑANA IREMOS AL CINE
- Texto cifrado: ANAÑAM SOMERI LA ENIC
- Código o algoritmo: hemos cambiado el orden de las letras en cada palabra
- Clave: en este caso no hay

Ahora completa tú el siguiente ejemplo siguiendo el modelo anterior:

- Texto plano: ME GUSTÓ MUCHO LA PELÍCULA
- Texto cifrado:.....
- Código o algoritmo:
- Clave:

CÓDIGO ATBAS: SE INVIERTE EL ORDEN DE LAS LETRAS EN EL ABECEDARIO

A	B	C	D	E	F	G	H	I	J	K	L	M	N
Z	Y	X	W	V	U	T	S	R	Q	P	O	Ñ	N

En este caso cada vez que debes escribir una de las letras escribes su asociada.

- Texto plano: MAÑANA IREMOS AL CINE
- Texto cifrado: NZMZNZ RIVÑLH ZO XRNV
- Código o algoritmo: hemos sustituido cada letra por su asociada

Ahora completa tú el siguiente ejemplo siguiendo el modelo anterior:

- Texto plano: ME GUSTÓ MUCHO LA PELÍCULA
- Texto cifrado:.....
- Código o algoritmo:

Muy bien, ya has visto como cifrar y descifrar mensajes. Vamos a seguir practicando.

Nivel 1. Aprendiendo a descifrar mensajes

Actividad. Aprendiendo a descifrar mensajes

En la siguiente actividad deberás descifrar un mensaje que ha sido encriptado con los siguientes símbolos y cifras:

a	b	c	d	e	f	g	h	i
Ⓐ	Ⓑ	Ⓒ	Ⓓ	Ⓔ	Ⓕ	Ⓖ	Ⓗ	①
j	k	l	m	n	ñ	o	p	q
①	②	③	④	⑤	⑦	⑥	⑦	⑧
r	s	t	u	v	w	x	y	z
⑨	⑩	①	②	③	④	⑤	⑥	⑥

Antes de empezar hagamos una prueba:

ㄣ5046 36 ㄣ6510ㄣㄣ109ㄣ10

--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

Y ahora deberás descifrar el siguiente mensaje oculto:

ㄣ3 1106 ㄣㄣ 3610 514ㄣ9610 ㄣ646
 3610 100306ㄣ4610 ㄣ65 ㄣ5 ㄣ0ㄣ

10ㄣ 9ㄣ4650ㄣ ㄣ ㄣㄣㄣㄣ 4ㄣ10 ㄣㄣ 10
 ㄣ010 403 ㄣ7610 ㄣ3 7905ㄣ0706 10
 ㄣ 110ㄣㄣㄣ5 3610 ㄣㄣㄣ610 ㄣㄣ 3ㄣ104ㄣ5
 610 ㄣ5 ㄣ3 ㄣ130026 ㄣㄣ 3ㄣ 00ㄣ9
 9ㄣ 5 ㄣ5 3610 5ㄣㄣ6ㄣ0610 ㄣ65 ㄣ
 504ㄣ3ㄣ10 ㄣ100ㄣ 100100ㄣ4ㄣ 10ㄣ 81ㄣ
 ㄣㄣㄣㄣ ㄣ6906 5 ㄣ47ㄣ66 ㄣ3 ㄣ650ㄣ
 6 ㄣㄣ 3610 514ㄣ9610 5ㄣ 10ㄣㄣ ㄣ65
 4ㄣ9ㄣㄣ10 ㄣㄣㄣㄣㄣ10

ㄣ5 15 0965ㄣ6 ㄣ65 51ㄣ610 6

ㄣ65 70ㄣㄣ9ㄣ10

Si has completado con éxito esta actividad ya has superado el Nivel 1. Aún deberás descifrar algunos mensajes encriptados más para convertirte en un experto en el arte de descifrar mensajes ocultos

Nivel 2. En busca del mensaje oculto...

Actividad. Descifra mensajes ocultos

Sabiendo que:

A	C	E	G	H	I	L	M
1	2	3	4	5	6	7	8
N	O	P	R	S	T	U	V
①	②	③	④	⑤	⑥	⑦	⑧

Busca en la siguiente Sopa de Números, ocho objetos que pondrás en la mesa para comer la sopa:

14⑦1

2⑦251④1 ⑤3④⑧6773⑥1 ③1①

81①⑥37

⑤②③3④1③71⑥②

⑧1⑤②

¿Qué objetos vas a poner en la mesa para comer la sopa? Escribe su nombre:

1	4	6	③	①	5	1	0	4	⑧
⑤	3	④	⑧	6	7	7	3	⑥	1
⑥	①	8	3	8	2	⑦	5	7	⑤
③	4	7	7	3	⑥	①	1	8	②
7	⑧	9	①	1	③	⑧	4	⑦	①
1	⑥	0	⑦	0	7	6	⑦	2	5
⑥	2	⑦	2	5	1	④	1	5	③
②	9	4	③	6	⑥	6	3	3	1
3	6	9	5	0	9	3	①	⑦	①
⑤	②	③	3	④	1	7	8	9	⑧

Si has completado con éxito esta actividad ya has alcanzado el Nivel 2

Nivel 3. Aprender a encriptar nuestros propios mensajes

Actividad. La escritura encriptada.

Creemos nuestro propio mensaje encriptado. Asigna (escribe o dibuja) un símbolo a cada letra para crear tu propio código:

A	B	C	D	E	F	G	H	I
J	K	L	M	N	Ñ	O	P	Q
R	S	T	U	V	W	X	Y	Z

Ahora escribe un mensaje utilizando los símbolos de tu código:

Cuando termines intercambia tu mensaje con el de un compañero o compañera e intentad descifrarlos utilizando el código creado.

Mensaje descifrado por tu compañero o compañera:

Si has completado con éxito esta actividad ya eres un experto en el arte de descubrir mensajes. ¡Enhorabuena!

Creamos nuestra propia máquina de encriptar mensajes

Actividad. Crear nuestro propio sistema de encriptado

En esta actividad deberás idear una máquina, código,... para cifrar mensajes. Hemos citado anteriormente algunos. Te mostramos algunos ejemplos que puedes utilizar pero también puedes idear tu propio sistema de encriptación.

Nombre del código de encriptación:	
Cómo funciona	
Haz un diseño de tu propuesta y explica cómo lo fabricarás	

A continuación te mostramos algunos ejemplos que te servirán para crear el tuyo.

Anexo I.

Modelo 1. Máquina de encriptar circular



Materiales necesarios:

- Ficha con tres círculos de diferente tamaño
- 1 fastener
- Tijeras y punzón.
- Regla.

Pasos:

Mide los tres círculos y marca el centro con un punzón. Recorta. Puedes plastificarlos si lo deseas.

Coloca el círculo pequeño sobre el mediano y éste sobre el grande y fíjalos con un fastener como éste:

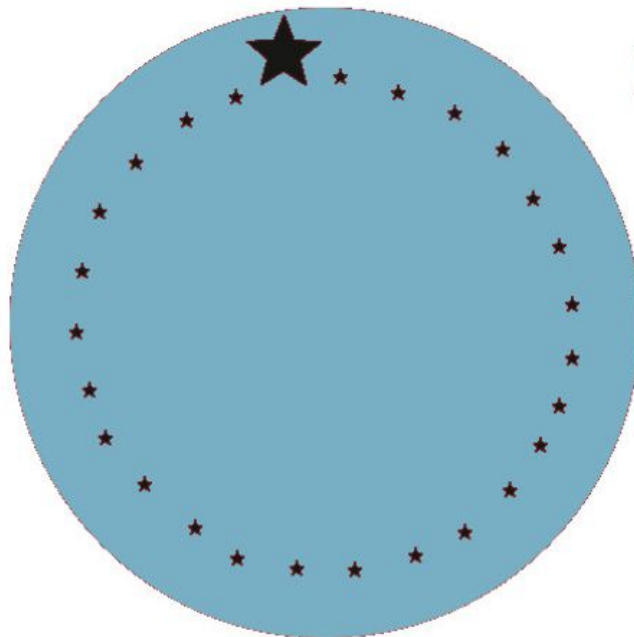
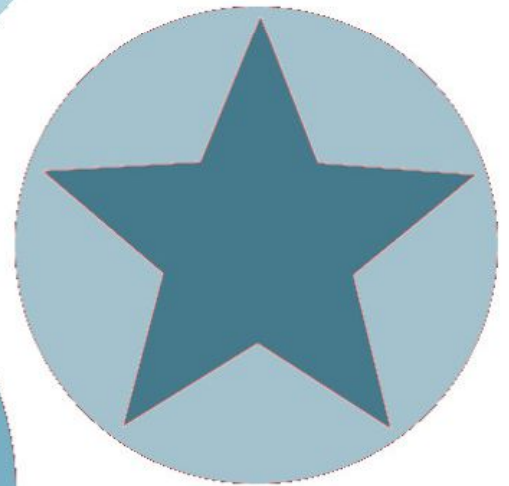
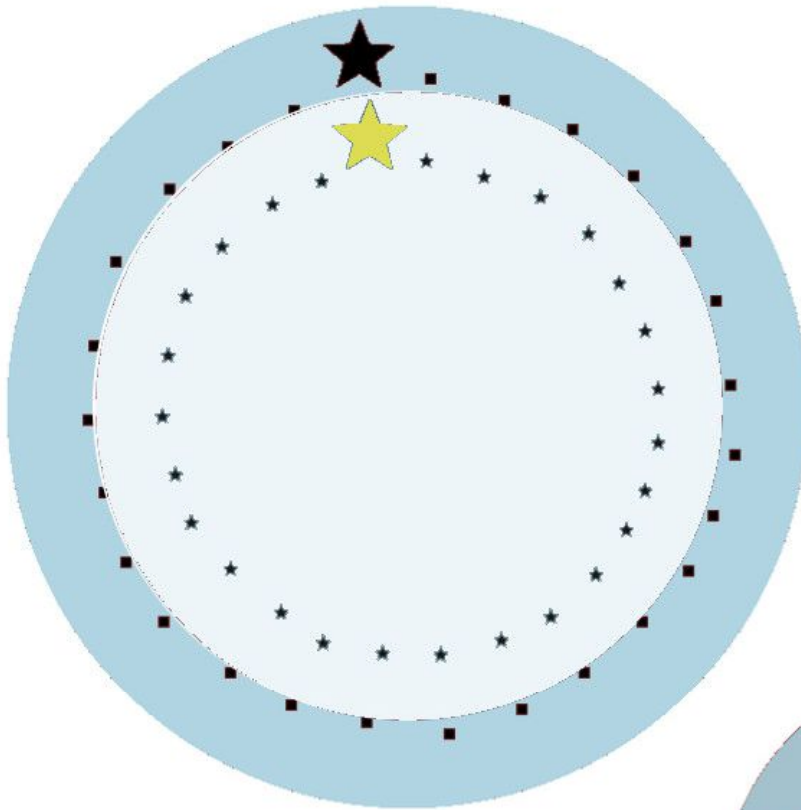


Escribe las letras del abecedario en cada una de las secciones del círculo más grande.

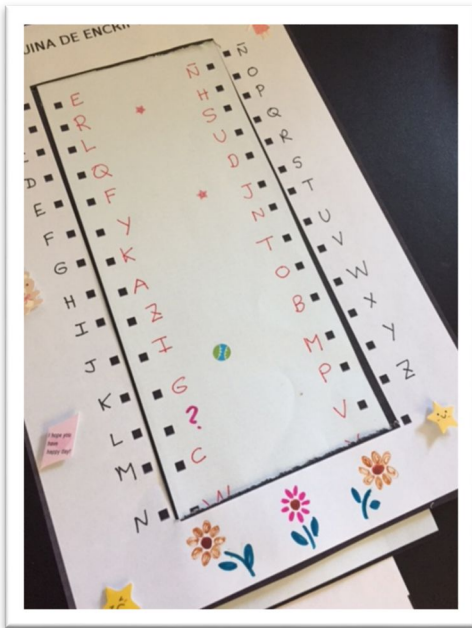
Escribe cada uno de los puntos del círculo mediano signos o símbolos. Si lo deseas puedes hacer varios códigos diferentes: con números, con letras, con signos, con imágenes...

¡Ya has creado tu primera máquina de encriptar! Escribe tu primer mensaje y pide a algún compañero que lo descifre. Recuerda que para que el mensaje solo pueda ser leído por vosotros dos deberéis compartir el código utilizado para encriptar.

MÁQUINA DE ENCRIPTAR MENSAJES



Modelo 2. Máquina de encriptar con cartulinas



Materiales necesarios:

- 2 Cartulinas de diferente color
- Rotuladores
- Tijeras

Pasos:

Haz un rectángulo de cartulina de 8 x 20 cm, dibuja una línea recta centrada y a 3 cm de su borde superior e inferior de unos 4 cm de ancho, perfora con la tijera y a continuación escribe en sus bordes las letras del abecedario tal como puedes ver en el modelo de la imagen.

A continuación corta otra tira de cartulina de 25 cm de largo por 4 cm de ancho, / de distinto color y escribe las letras del abecedario en sus bordes pero de forma desordenada (También puedes utilizar signos o símbolos).

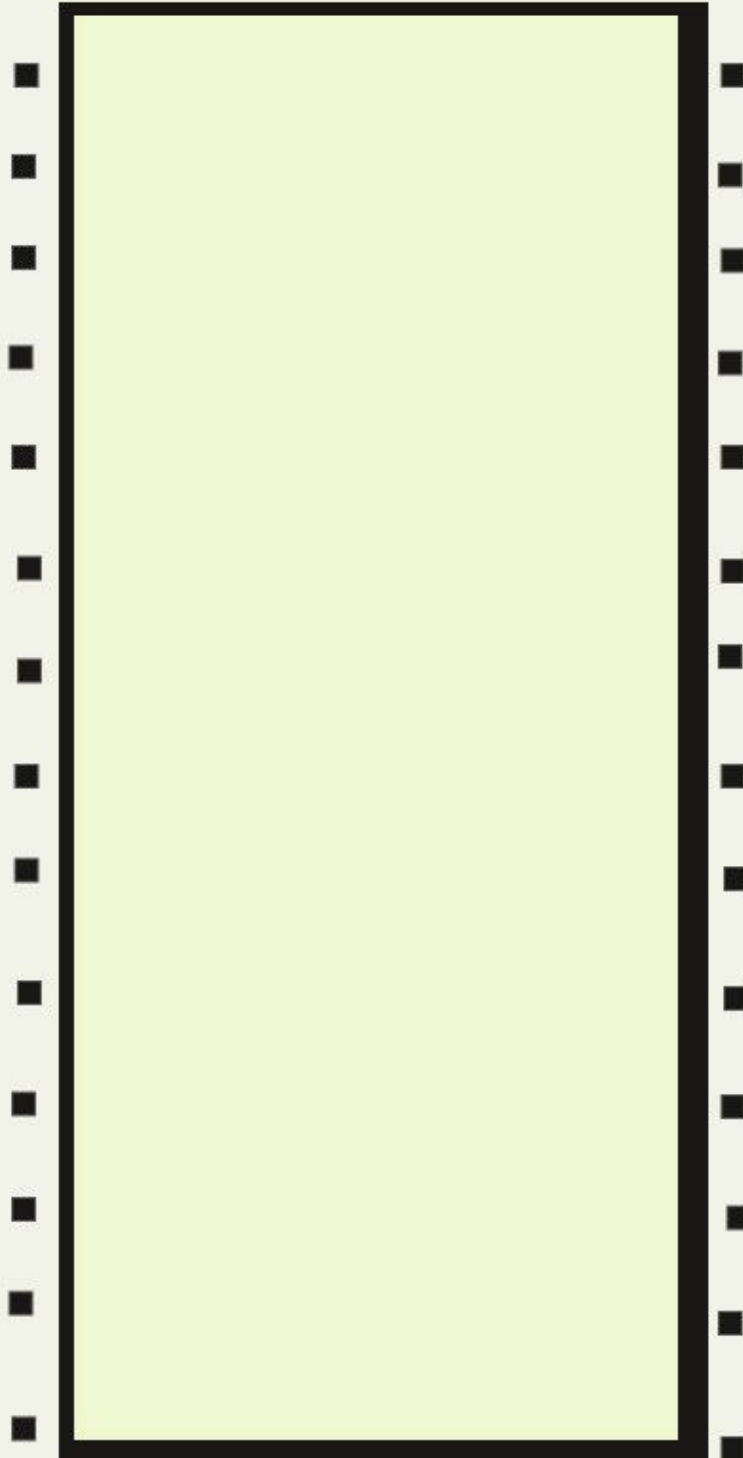
Pasa la tira más estrecha por las dos ranuras del rectángulo procurando que deslice bien.

A continuación tienes un modelo que puedes utilizar.

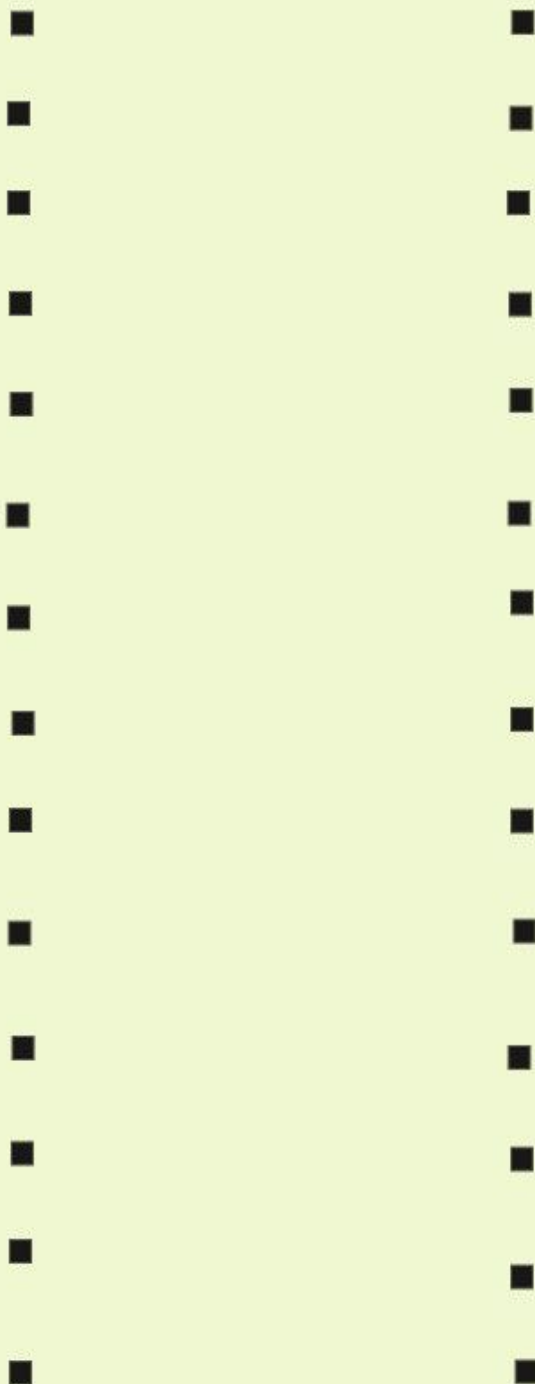
Decora tu codificador como prefieras. Puedes utilizar dibujos, fotografías, pegatinas...

¡Ya has creado tu máquina de encriptar! Escribe tu primer mensaje y pide a algún compañero que lo descifre.

MÁQUINA DE ENCRIPtar MENSAJES



CÓDIGO DE ENCRIPtar



Para aprender más sobre los mensajes encriptados

Actividad. ¿Qué es la criptografía?

Escribe lo que sepas sobre los siguientes sistemas de encriptación y explica en qué consisten:

